

EX PARTE C

FILE

ORIGINAL

1301 K Street N.W.
Washington, DC 20005-3307

October 3, 2003

EX PARTE OR LATE FILED

Ms. Marlene H. Dortch
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

RECEIVED

OCT - 8 2003

Re *Ex Parte* presentation in MB Docket No. 02-230FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Dear Ms. Dortch

On October 2, 2003, Jeff Lotspiech, Don Leake, Cheryl Bruner, and Sally Lake of IBM Corporation met with the following staff of the FCC's Media Bureau and Office of Strategic Planning and Policy Analysis:

Rick Chessen
Alison Greenwald
John Wong
Tom HoranBill Johnson
Amy Nathan
Jonathan Levy
Maureen McLoughlin

The purpose of the meeting was to introduce the FCC to xCP (for "extensible content protection"), an IBM encryption technology which can be used to secure digital terrestrial broadcast content. IBM presented written material, two copies of which are attached, to the meeting participants.

In addition to presenting the written material, IBM made the following points:

xCP is a form of "broadcast" encryption technology evolved from CPRM¹. CPRM is an approved output of DTCP² which is becoming widely accepted as content protection for physical media. Both CPRM and xCP are relevant to a Broadcast Flag regime, and would hypothetically be technologies to include on "Table A". It is important that reasonable, objective criteria be established to guide the development of content protection technologies required as part of the Broadcast Flag regime. A transparent process of self-certification would be most efficient for qualifying technologies to "Table A". There are strong precedents in the IT industry for effective self-certification. This process was used successfully for homologation and emission testing – both instances where failure to comply would make devices work poorly or not at all.

"Broadcast" encryption is a cryptographic term that describes a specific type of encryption that does not require an exchange of information between devices. xCP allows circumventing devices to be selectively eliminated (have their keys revoked), without

¹ CPRM stands for Content Protection for Recordable Media

² DTCP stands for Digital Transmission Content Protection

No. of Copies rec'd 01/
List A B C D E

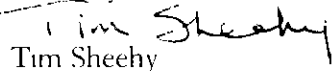
affecting compliant devices. Response to a broken key set is two part: In the case of pre-recorded media, the time period between the break and key renewal is completely under the control of the content owner, who can trade off the cost of remastering his content against the seriousness of the attack. In the case of blank recordable media, the media manufacturer is obligated by his license to update his media when new revocation is required. He is allowed some lead time, so his manufacturing process can remain efficient. The tree system employed by xCP provides billions of keys - more than the total number of devices manufactured during the life of the system. This helps reduce the cost of providing copy protection. The renewability of xCP is very attractive to content owners - the system can not be made useless by one or even many clever hackers, who might be colluding. While IBM believes the standard definition of "home network" remains to be worked out among all stakeholders, the design of xCP allows a policy decision by the stakeholders to specify the number of devices which would be part of the system.

xCP can be thought of as one component of a full service digital rights management system (DRM). Full-service DRM has end-to-end coverage of the system through which the data flows. Support functions such as content protection tools, website function from which content can be sold or licensed, clearinghouse function or a licensing server which approves the purchase or license of content, and a content server where content is stored before it is sold are also features. xCP is well suited to be a part of a DRM system.

IBM has a long history of doing leading research in cryptography. This research led to the creation of the Data Encryption Standard (DES), which has been an international standard for many years. The copy protection technology developed by IBM responds to the needs of customers, many of whom are in the content business. Copy protection activity in the Media and Entertainment industry is serving as an incubator for technology applications which can be used across a wide variety of industry sectors where privacy or confidentiality are important issues.

In accordance with Section 1.1206 of the Federal Communications Commission Rules, this original and one copy are provided to your office. A copy of this letter is being delivered to each of the FCC parties listed above.

Sincerely,



Tim Sheehy
Director, Public Policy

cc. Rick Chessen
Alison Greenwald
John Wong
Tom Horan
Bill Johnson
Amy Nathan
Johnathan Levy
Maureen McLoughlin

xCP Presentation to the FCC

Purpose of the meeting: Introduce the FCC to xCP, an encryption technology that can secure broadcast flag marked content

From IBM's letter to the FCC (February, 2003) on the Broadcast Flag:

Secure Home Networks are technically feasible and should be flexible:

IBM believes the notion of establishing a logical Home Network is technically feasible. IBM specifically has been working on technologies that enable authorized domains. In particular, IBM has submitted a new encryption technology (xCP) to the Digital Video Broadcast (DVB) standards body - the European body currently developing standards for Home Networking. This technology is consistent and compatible with the approach used in the 4C solution, and provides consumers with the capacity to take their home network licensed content away from home on portable media. IBM believes this technology can be made to work in concert with other technologies to create an environment where authorized content can move in a flexible use model and enable new business models for content companies, consumer device producers and service providers.

xCP Presentation to the FCC

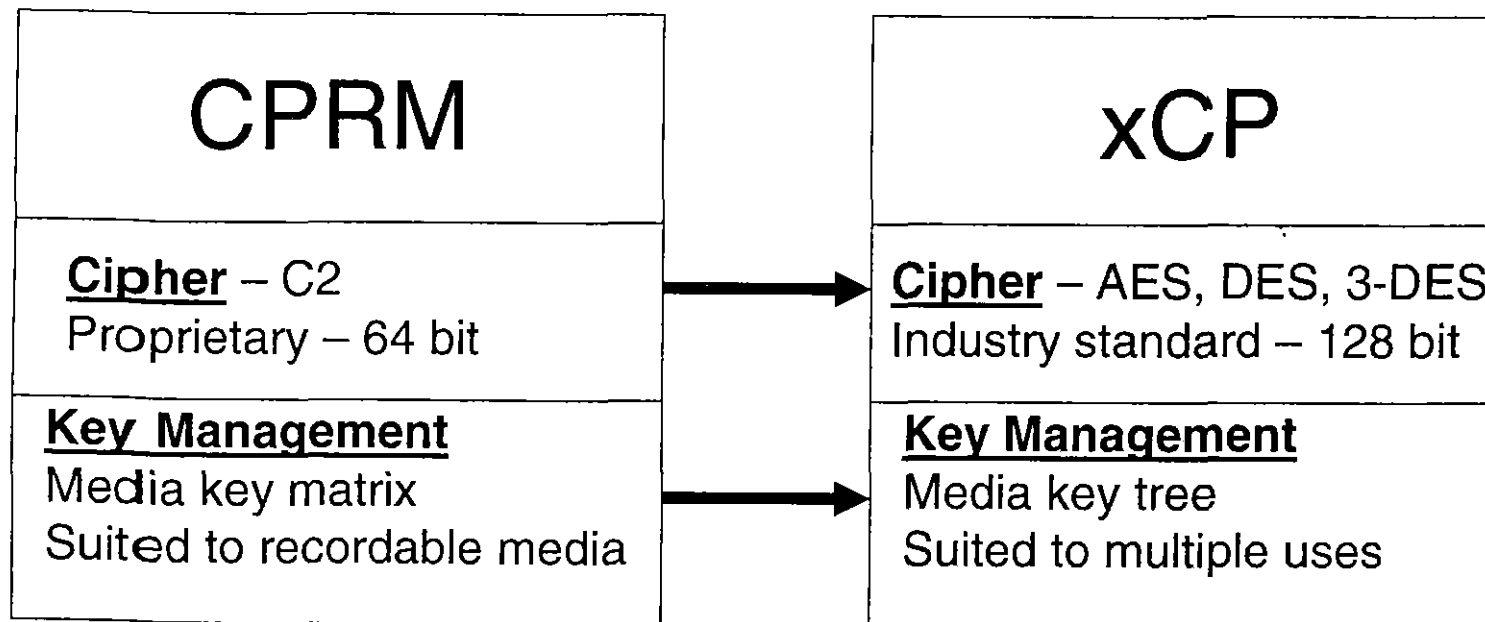
- Some Notes for Clarity and Understanding:
 - While IBM is making some bold assertions, we realize that the FCC does not have to accept them
 - IBM is making this presentation in the interest of making progress in protecting copyright content
 - IBM fully realizes that the term “Table A” is an artifact of the BPDG Report and that the approved list of technologies will probably be called something different
 - IBM also fully realizes that the FCC will develop a Table A process that is fully transparent
 - This presentation is not an attempt to circumvent any such process
 - Several content organizations recommended that IBM make the FCC aware of xCP and its capabilities

xCP Presentation to the FCC

- xCP is a broadcast encryption technology, that is an evolution of 4C CPRM
- xCP can be used to secure content in multiple media types:
 - Portable, writable, physical media
 - (writable DVD, memory cards, mini-disks)
 - Wide area networks
 - Home networks

xCP Presentation to the FCC

- xCP is an evolution of 4C CPRM and should be included on Table A
 - Cipher now an international industry standard
 - Key management space has been expanded



xCP Presentation to the FCC

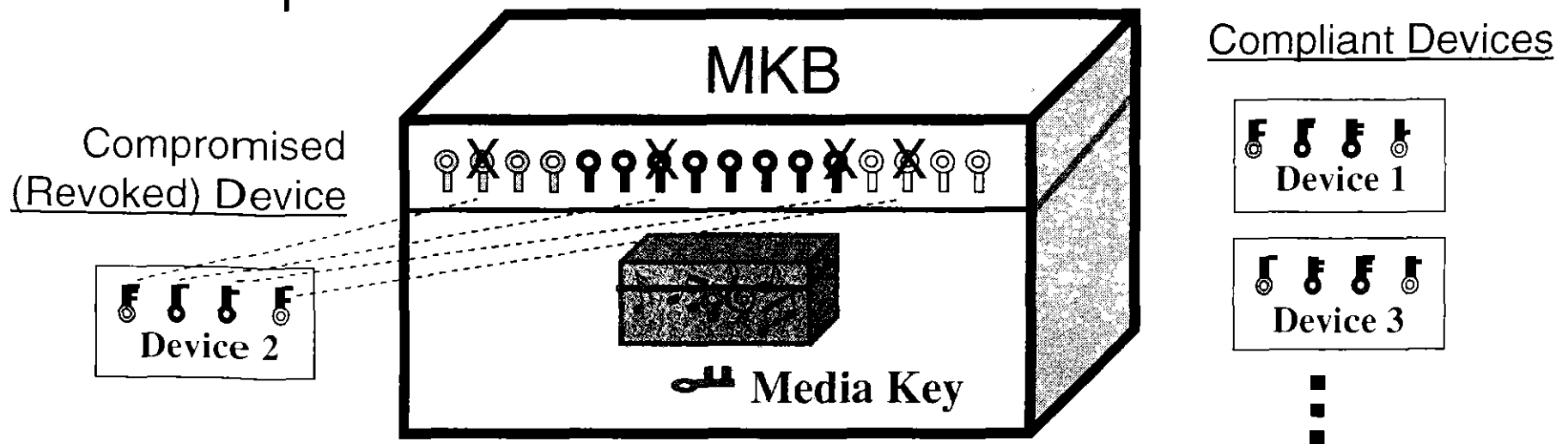
- CPRM may become part of Table A as an approved output of DTCP
- CPRM is a well accepted encryption technology, even though it may not meet all of the proposed criteria
 - Over XXX licensees, including most major CE companies
 - Over YYY licenses in force
 - Over ZZZ million devices implemented with CPRM
 - Warner Music Group and Universal Music Group are licensed content participants
 - 6 major Japanese record companies have recently announced that they will release 100 new DVD Audio titles that will be protected by the version of CPRM for pre-packaged content
- Since xCP is an evolution of CPRM, but can be used to protect a broader menu of media types, it should also be considered for inclusion on Table A

“Broadcast Encryption”

- Refers to *one-way* key management (key management without a handshake)
 - As opposed to a public-key based system.
- Like CPRM before it, xCP is fundamentally based on a broadcast encryption
 - New (Crypto 2000) tree-based media key block; equivalent in revocation power to public key
 - Automatically protects storage
 - Storage devices do not have to participate; e.g., “Internet locker” allowed

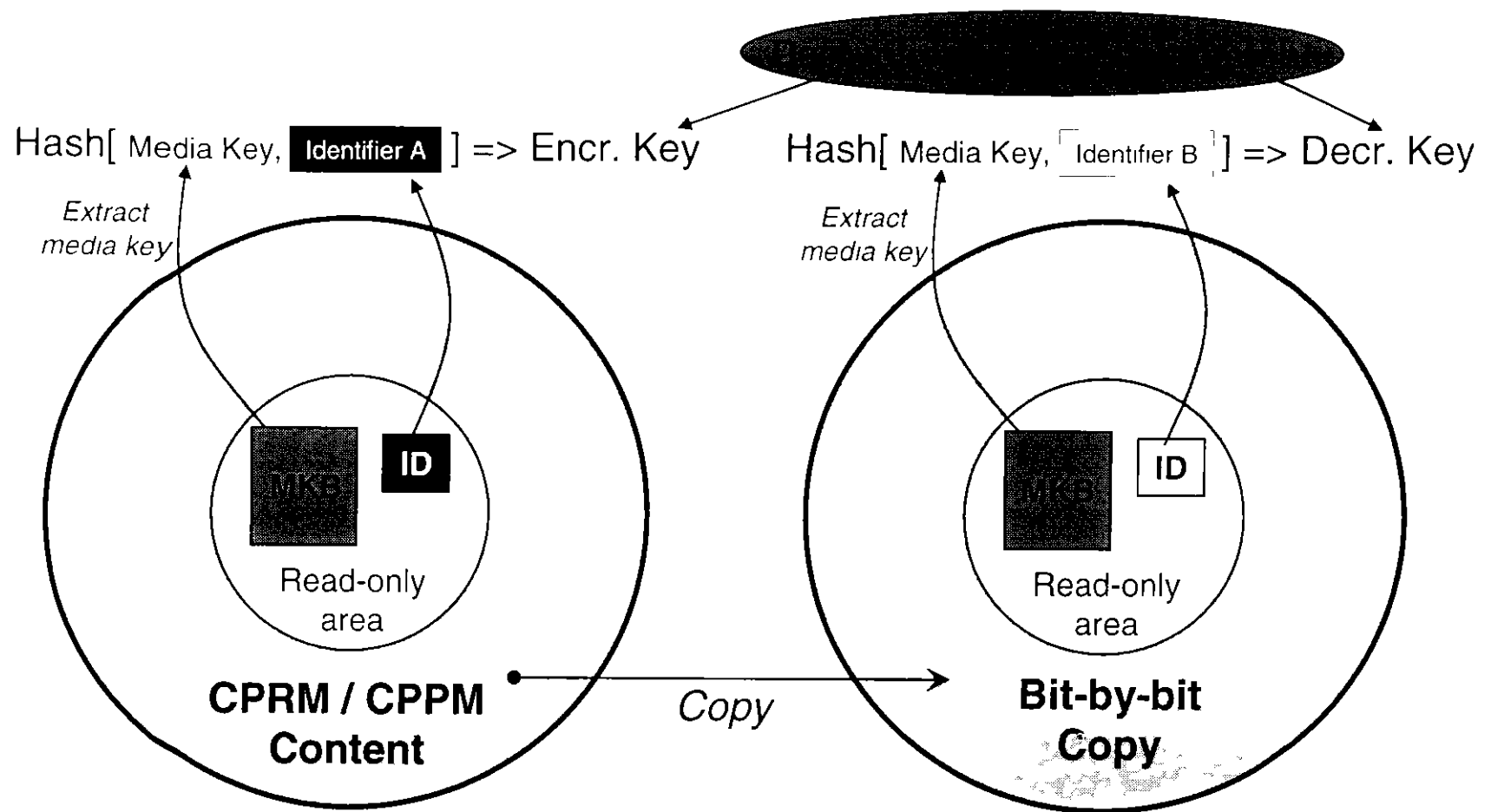
System Renewability

- Each device assigned individual set of keys
- Revocation of compromised keys
 - Allows compliant devices to calculate secret “Media Key”
 - Revoked keys calculate incorrect Media Key
- MKB periodically updated (through broadcast and pre-recorded media)



Bit-by-bit Copies

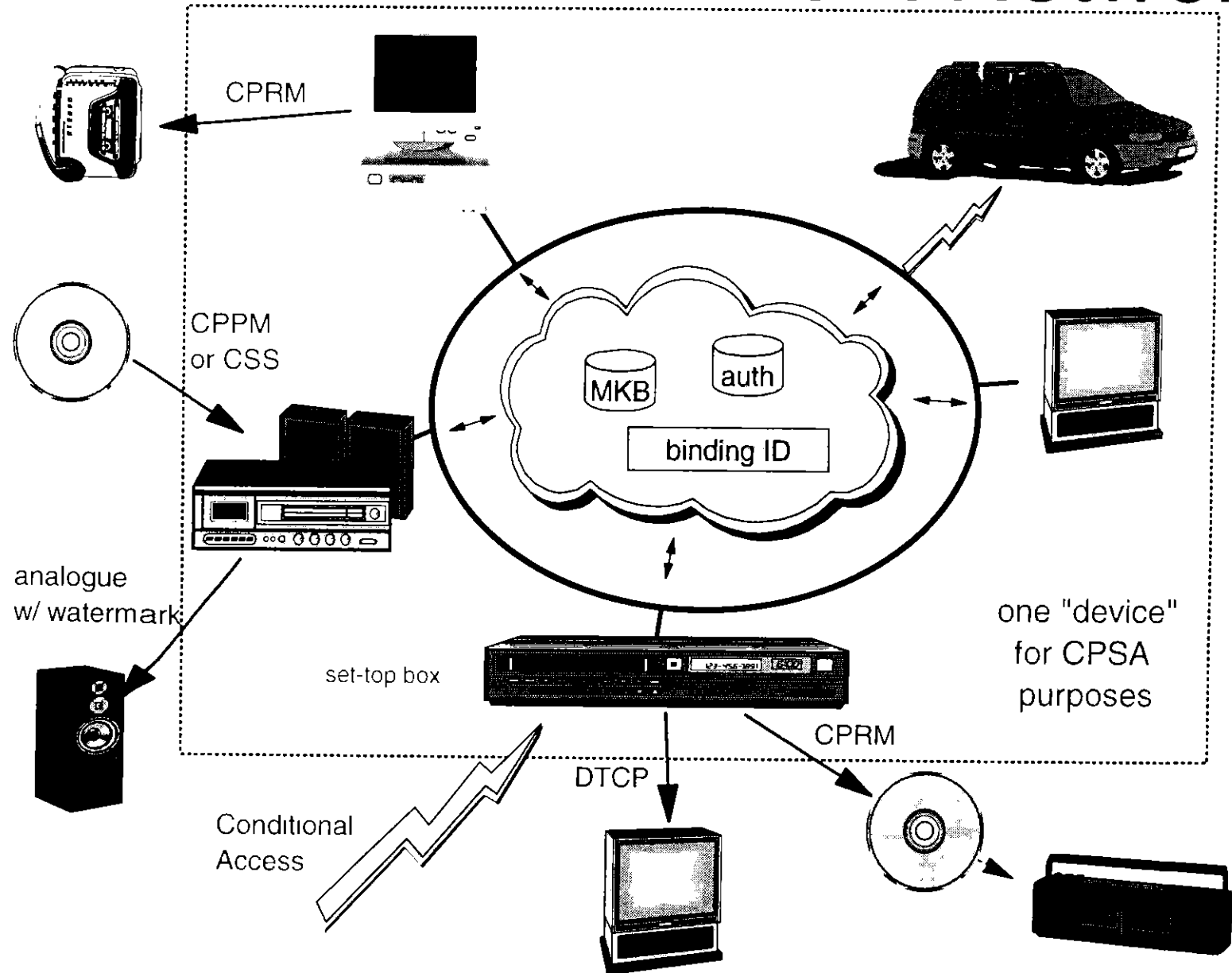
- Use of identifier in determining key ensures that bit-by-bit copies won't play



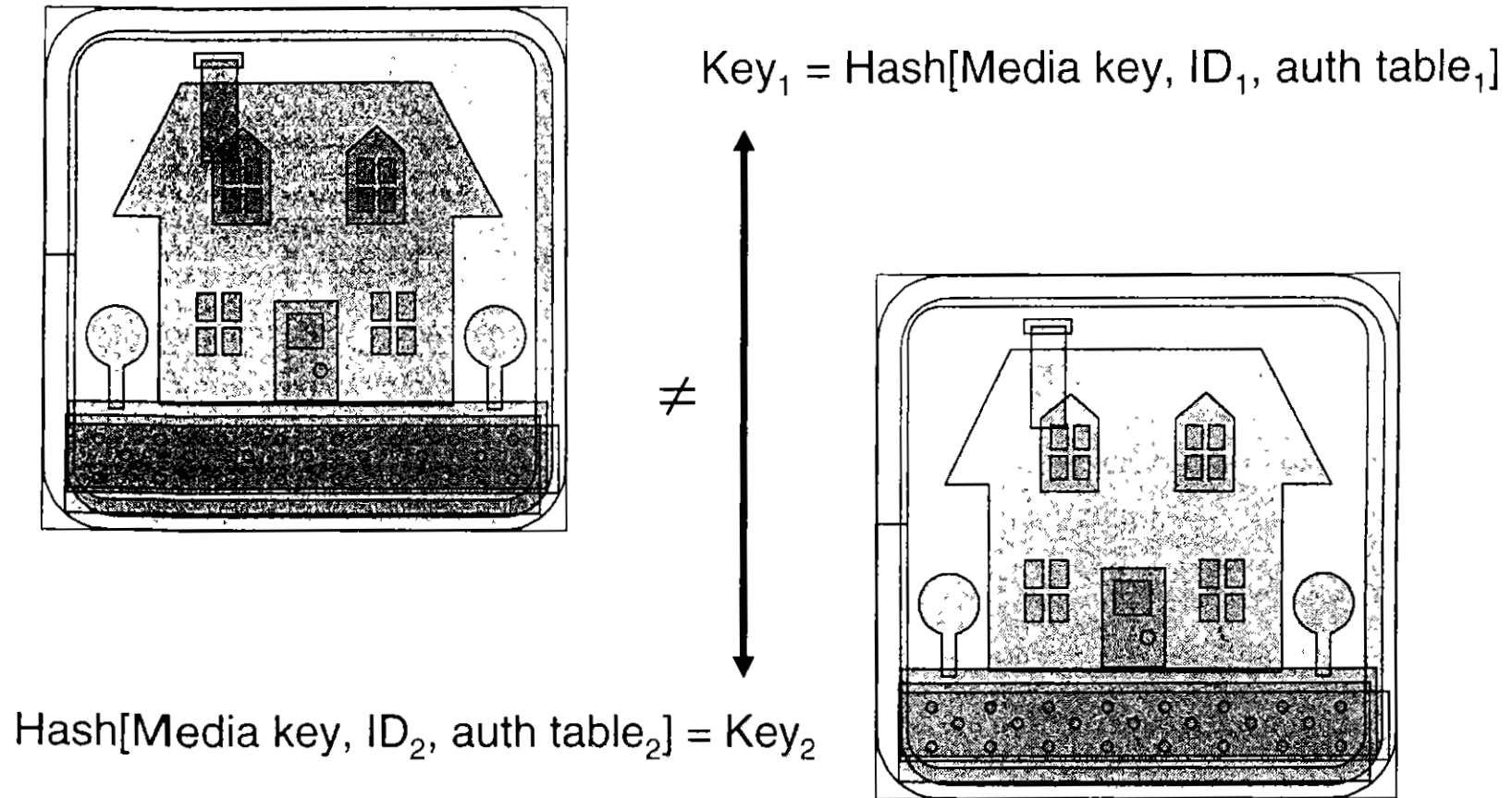
IBM's Perspective on Home Networking

- Today, there are two types of content protection schema's
 - Point solutions – watermarking, analog copy protection
 - DRM systems – EMMS, Windows Media, Real
- Neither of these satisfies the requirements for end-to-end content security
- IBM is offering the following concept:
 - Architected end-to-end solution
 - Open interfaces
 - Governed by licensing
 - Multiple content protection technologies
 - Compute efficient client solution based on broadcast encryption

Home Entertainment Network

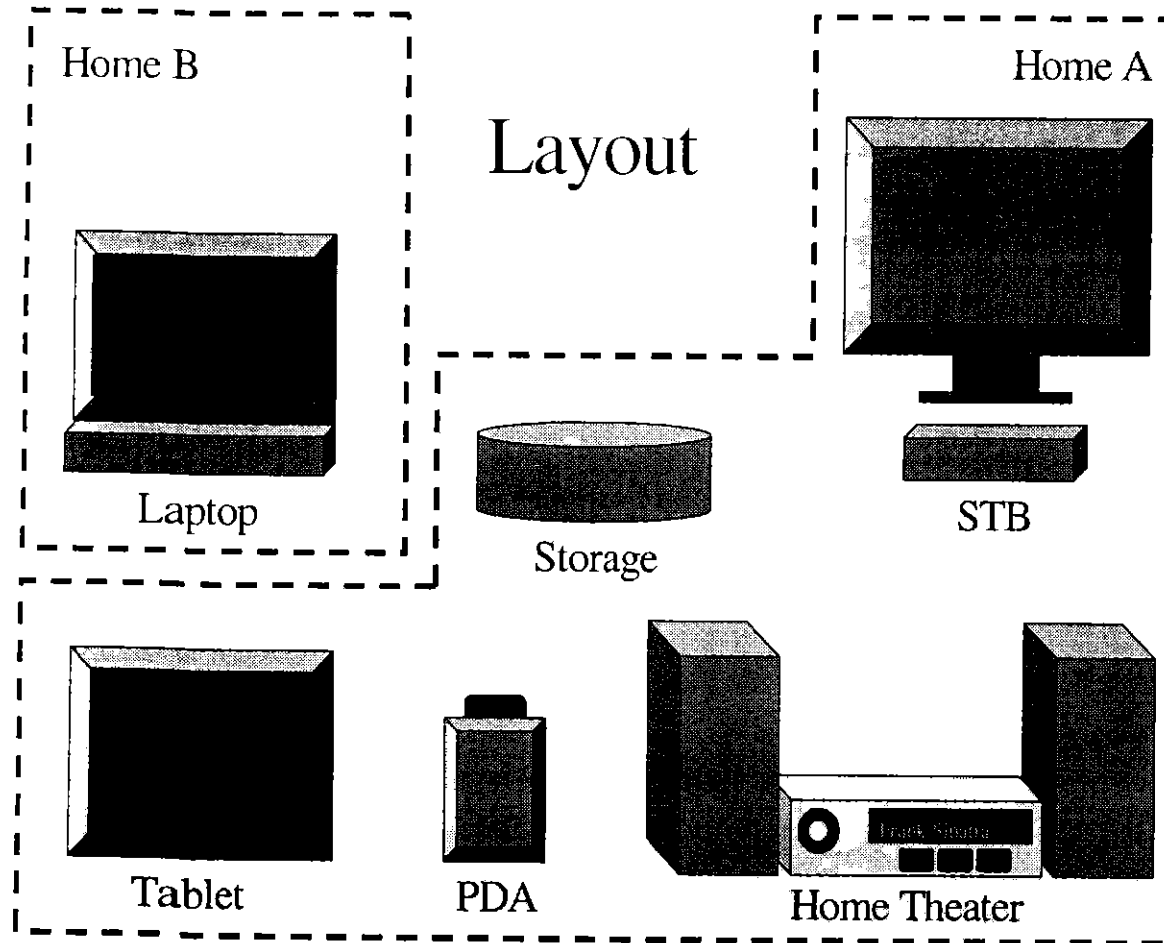


Two Home Networks



Just like CPRM prevents bit-for-bit copies of media, xCP prevents two homes from sharing their content.

IBM Home Networking Demo at NAB 2003



Scenarios:

1. Cluster bootstrap
2. Content playback
3. Device join
4. Playback attempt outside cluster
5. Non-compliant device join attempt
6. Download new content
7. Revocation information update

2 & 4: 1 minute demo

1-5: 5 minute demo

1-7: 15 minute demo

Summary

- xCP is a very versatile and powerful encryption technology for use with physical media, wide area networks and home networks
- xCP is an evolution of CPRM which is well vetted in the marketplace
 - Uses international standard ciphers
 - Expands the key space
- xCP is highly thought of by the content community
- There should be an efficient way of getting technologies like xCP on Table A

IBM xCP – Fact Sheet

Background:

With the advent of consumer grade digital technology, content such as music and movies are no longer bound to the physical media that carries it. This advent presents new challenges to content owners – record labels, studios, distribution networks and artists – who want to protect their intellectual property from indiscriminate reproduction and distribution while at the same time extracting economic benefits from this content

IBM Research has developed a powerful and flexible content protection system code-named xCP (eXtensible Content Protection) that has many potential uses, but is especially appropriate for home networks. xCP is consistent with IBM's content protection system architecture (CPSA). The technology is based on Broadcast Encryption and supports the notion of a trusted domain that groups together several compliant devices. Content can move freely among these devices, but it is useless to devices located outside of the domain. xCP provides a cryptographically strong, yet extremely flexible model for access to copy-protected content within a home network.

Technology Overview:

xCP provides a security architecture for digital media whether electronic or physical, and could support many new formats

xCP provides the security architecture to create home networks which allow authorized content portability within a home domain and across various authorized consumer devices.

xCP can be linked with IBM Web Services technology to provide a platform to link the necessary services to tie together physical media and the logical network architectures, enabling commerce. Security and commerce can be linked together in a new content ecosystem that does not require large client side architectures

xCP is a Cluster Protocol for broadcast encryption that uses a media key block system, and marks the first time that broadcast encryption technology has been used in a peer-to-peer application. The technology requires little or no Internet connectivity and works by allowing all of the devices within a "home" network to establish common media keys. These unique IDs distinguish each device in the network from other devices, thereby preventing use (viewing or listening) of the content by devices outside the network

xCP Features:

xCP supports plug-n-play functionality, without requiring user intervention, for a limited number of devices. For example, a user might play content seamlessly on his home theater in one room of a house. When a wireless audio player, for example, is purchased for use in another room in the house, this new device automatically joins the domain and has access to the existing content

xCP users have the option of managing their domain, restricting who can join, removing devices or requesting extensions to the trusted domain to incorporate additional devices.

xCP supports intermittently-connected devices and does not require online access to central servers for playback, enabling a wide range of consumer electronic devices to participate in the domain.

xCP allows content owners to retain control over the distribution of content. If a user's friend were to download some of the user's files, the content would not work on the friend's player without first acquiring an additional license.

xCP allows for the joining and splitting of domains due to marriage/divorce, sharing content across a main residence and a summer home, download/playback on mobile devices including cell phones, PDAs, Internet-based storage lockers and Personal Video Recorders.

Relationship of xCP Cluster to the Copy Protection System Architecture:

